# INSPECTOR GENERAL

U.S. Department of Defense

DECEMBER 13, 2016

DoD Cybersecurity Weaknesses as Reported in Audit Reports Issued From August 1, 2015, Through July 31, 2016
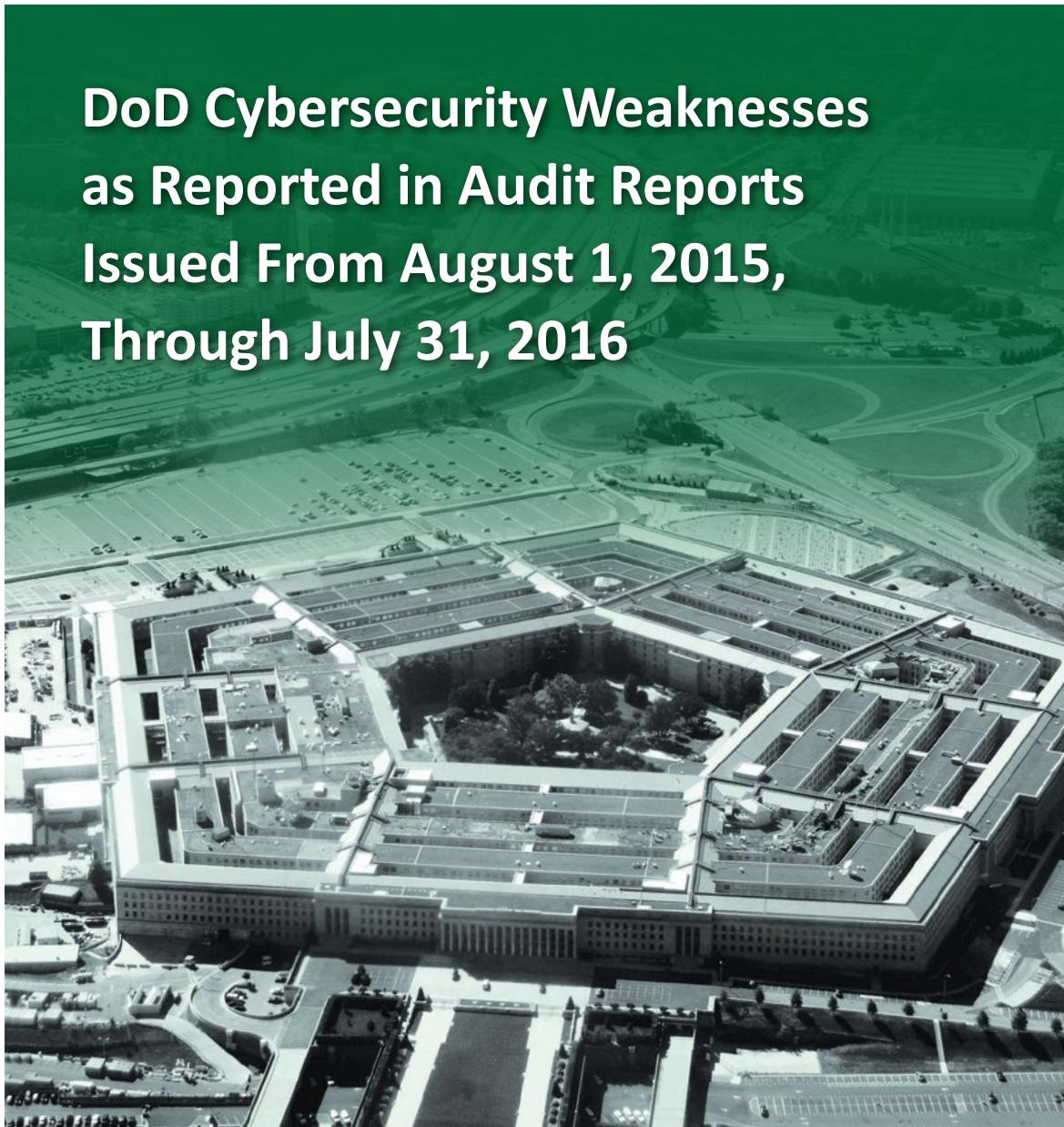
INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Mission

Our mission is to provide independent, relevant, and timely oversight of the Department of Defense that supports the warfighter; promotes accountability, integrity, and efficiency; advises the Secretary of Defense and Congress; and informs the public.

Vision

Our vision is to be a model oversight organization in the Federal Government by leading change, speaking truth, and promoting excellence—a diverse organization, working together as one professional team, recognized as leaders in our field.

Fraud, Waste, & Abuse
HOTLINE
Department of Defense
dodig.mil/hotline | 800.424.9098

For more information about whistleblower protection, please see the inside back cover.

Results in Brief

DoD Cybersecurity Weaknesses as Reported in Audit Reports Issued From August 1, 2015, Through July 31, 2016

December 13, 2016

Objective

We summarized DoD and Government Accountability Office audit reports issued from August 1, 2015, through July 31, 2016, that contained findings on DoD cybersecurity weaknesses. This report supports the DoD Office of Inspector General's response to the requirements of Public Law 113-283, section 3555, "Federal Information Security Modernization Act of 2014," December 18, 2014.

Results

During the reporting period, the DoD and the Government Accountability Office issued 21 unclassified reports that addressed a wide range of cybersecurity weaknesses within the DoD systems and networks. Reports issued during the reporting period most frequently cited cybersecurity weaknesses in the categories of risk management, identity and access management, security and privacy training, contractor systems, and configuration management.

As of August 1, 2015, unclassified audit reports identified in the previously issued cybersecurity summary reports contained 166 open cybersecurity-related recommendations. From August 1, 2015, through July 31, 2016, DoD management closed 28 recommendations, leaving 138 open cybersecurity-related recommendations that required management action.

Results (cont'd)

The DoD has prioritized funding its cyber strategy by investing a total of $6.7 billion in FY 2017 and a total of $34.6 billion over the Future Years Defense Program (next five years). The funds are intended to help the DoD continue to develop, train, and equip the Cyber Mission Force, and make new technological investments to strengthen cyber defenses and capabilities. While the DoD has prioritized funding its cyber strategy, cybersecurity will continue to remain a significant management challenge. As recent audit reports identify, the DoD continues to struggle with ensuring that all aspects of its information security program are adequately implemented. For example, implementing secure information systems on major weapons systems throughout their lifecycle requires effective and continuous software assurance testing. Inadequate software assurance testing on major weapons systems could be devastating to mission operations. In addition, although Homeland Security Presidential Directive 12 was issued in 2004, one audit report indicated that DoD Components are still not fully complying with the Directive. The report identified the lack of compliance leaves national security and Privacy Act information vulnerable to compromise and places soldiers, family members, civilians, and critical infrastructures at greater risk of an adverse incident occurring.

Correcting cybersecurity weaknesses and maintaining adequate cybersecurity is critical, as the DoD has become increasingly reliant on cyberspace to enable its military, intelligence, and business operations to perform the full spectrum of military operations. Although the DoD has taken steps to increase cybersecurity over its systems, networks, and infrastructure, significant challenges remain.

Visit us at www.dodig.mil

Results in Brief

DoD Cybersecurity Weaknesses as Reported in Audit Reports Issued From August 1, 2015, Through July 31, 2016

Recommendations

In this summary report, we identified recommendations from previously issued reports. Therefore, this report contains no new recommendations and is provided for information purposes only.

Management Comments and Our Response

We did not issue a draft report because this report consolidates audit findings from audit reports issued from August 1, 2015, through July 31, 2016. No written response is required.

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

December 13, 2016

MEMORANDUM FOR DOD CHIEF INFORMATION OFFICER
      ASSISTANT SECRETARY OF THE AIR FORCE
        (FINANCIAL MANAGEMENT AND COMPTROLLER)
      NAVAL INSPECTOR GENERAL
      AUDITOR GENERAL, DEPARTMENT OF THE ARMY
      MANAGING DIRECTOR, INFORMATION TECHNOLOGY,
        GOVERNMENT ACCOUNTABILITY OFFICE

SUBJECT: DoD Cybersecurity Weaknesses as Reported in Audit Reports Issued From
        August 1, 2015, Through July 31, 2016 (Report No. DODIG-2017-034)

We are providing this summary report for your information and use. Civil service and
military personnel who develop, operate, or manage DoD information systems should read this
report to be aware of identified cybersecurity challenges in the DoD information technology
environment. The overall objective was to summarize the DoD cybersecurity weaknesses
identified in unclassified audit reports and testimonies issued by the DoD audit community
and the Government Accountability Office from August 1, 2015, through July 31, 2016. During
the reporting period, the DoD audit community and the Government Accountability Office
issued 21 unclassified reports addressing cybersecurity weaknesses within DoD systems
and networks.

The report contains no recommendations for action; however, it does identify previously
issued audit reports that contain open recommendations. We did not issue a draft report,
and no written response is required.

We appreciate the courtesies extended to the staff. Please direct questions to me at
(703) 699-7331 (DSN 499-7331).

Carol N. Gorman
Assistant Inspector General
Readiness and Cyber Operations

Contents

Introduction

Objective

We summarized DoD cybersecurity weaknesses identified in audit reports and testimonies issued by the DoD audit community[1] and the Government Accountability Office (GAO) between August 1, 2015, through July 31, 2016. See Appendix A for a discussion on the scope and methodology and prior coverage related to the objective.

Background

This report is the 18th annual cybersecurity summary the DoD Office of Inspector General (DoD OIG) has issued since January 1999. This report is a reference for identifying audit reports and testimonies that outline DoD cybersecurity weaknesses as related to Public Law 113-283, section 3555, "Federal Information Security Modernization Act of 2014 (FISMA)," December 18, 2014.[2]

FISMA Requires Security Controls Over Federal Information

Federal Government agencies have a responsibility to protect their information and information systems. This responsibility is promulgated in FISMA, which provides a comprehensive framework for ensuring the effectiveness of agency information security controls. FISMA requires that each agency develop, document, and implement an agency-wide information security program to protect the information and information systems that support agency operations and assets. FISMA also requires that each agency with an Inspector General (IG) appointed under the Inspector General Act of 1978, as amended, independently evaluate the effectiveness of the agency's information security program and practices.

Due to the size and number of DoD organizations, a comprehensive annual evaluation of the DoD's information security program for each of the FISMA metrics is not practical. Instead, the DoD OIG uses this summary of unclassified cybersecurity-related audit reports and testimonies issued by the DoD audit community and the GAO during the reporting period to support the DoD OIG's annual FISMA requirement.

---

[1] The DoD audit community consists of the DoD Office of Inspector General, Army Audit Agency, Naval Audit Service, and Air Force Audit Agency.

[2] The Federal Information Security Modernization Act of 2014 amends the Federal Information Security Management Act of 2002.

Cybersecurity Weakness Categories

In 2010, the Office of Management and Budget mandated that the Department of Homeland Security provide guidance and operational oversight for Federal agency FISMA reporting. In accordance with that mandate, the Department of Homeland Security has developed and issued annual FISMA reporting metrics for Federal agency IGs, Chief Information Officers, and the Senior Agency Officials for Privacy. This year, the Office of Management and Budget, the Department of Homeland Security, and the Council of the Inspectors General on Integrity and Efficiency established a joint working group to develop the FY 2016 IG FISMA reporting metrics. The FY 2016 IG FISMA metrics are defined in "FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics, V1.0," June 20, 2016.

The FY 2016 IG FISMA metrics are organized around the five information security functions outlined in the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework). The five security functions are Identify, Protect, Detect, Respond, and Recover. The Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the agency and provides IGs with guidance for assessing the maturity of the controls to address those risks. Table 1 shows the eight FY 2016 IG FISMA reporting metrics and their alignment to the Cybersecurity Framework security functions.

Table 1. FY 2016 IG FISMA Reporting Metrics

Cybersecurity Framework Security Functions	FY 2016 IG FISMA Reporting Metrics
Identify	Risk Management
	Contractor Systems
Protect	Configuration Management
	Identity and Access Management
	Security and Privacy Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

Based on their respective set of metrics, the IGs, Chief Information Officers, and Senior Agency Officials for Privacy assess their agency information security controls and compile the results in a single FISMA assessment report to the Office of Management and Budget. The annual reports are submitted electronically in CyberScope, an automated platform for secure FISMA reporting.

To respond to the FISMA requirements, the DoD OIG categorizes the cybersecurity-related audit report and testimony findings by cybersecurity weakness categories, consistent with the eight FY 2016 IG FISMA reporting metrics. See the Glossary for definitions of each cybersecurity weakness category.

DoD Cybersecurity Instructions and Directives

The DoD has issued the following cybersecurity guidance, which is consistent with the FISMA reporting metrics.

- DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, establishes a DoD cybersecurity program to protect and defend DoD information and information technology (IT).

- DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014, Incorporating Change 1, May 24, 2016, establishes policy and assigns responsibility for executing and maintaining the DoD IT risk management framework. This policy provides guidance for the transition from the DoD Information Assurance Certification and Accreditation Process to the risk management framework.

- DoD Instruction 8582.01, "Security of Unclassified DoD Information on Non-DoD Information Systems," June 6, 2012, establishes policy for securing unclassified information on non-DoD information systems.

- DoD Instruction 8520.03, "Identity Authentication for Information Systems," May 13, 2011, establishes policy and prescribes procedures for implementing identity authentication of all entities to DoD information systems.

- DoD Directive 5400.11, "DoD Privacy Program," October 29, 2014, establishes policy for the respect and protection of an individual's personal information and fundamental right to privacy.

- DoD Directive 8140.01, "Cyberspace Workforce Management," August 11, 2015, establishes specific workforce elements to align, manage, and standardize cyberspace work roles, baseline qualifications, and training requirements.

Results

DoD Audit Community and GAO Identified DoD Cybersecurity Weaknesses

From August 1, 2015, through July 31, 2016, the DoD audit community and the GAO issued 21 unclassified reports that identified a wide range of cybersecurity weaknesses within DoD systems and networks. The reports identified issues in seven of the eight IG FISMA metrics. The DoD audit community and the GAO provided 61 recommendations related to the FY 2016 IG FISMA metrics to correct cybersecurity weaknesses.

Cybersecurity Weaknesses Identified in Audit Reports

This report summarizes the cybersecurity weaknesses identified in DoD audit community and GAO reports as they relate to the FY 2016 IG FISMA metrics. Table 2 shows the number of cybersecurity weaknesses related to the FY 2016 IG FISMA reporting metrics identified in the 21 reports.

Table 2. Cybersecurity Weaknesses Reported From August 1, 2015, Through July 31, 2016

FISMA Reporting Metrics	GAO	DoD OIG	Military Departments	Total
Risk Management	1	4	8	13
Identity and Access Management	0	1	4	5
Security and Privacy Training	0	0	5	5
Contractor Systems	2	1	1	4
Contingency Planning	0	0	3	3
Configuration Management	0	1	2	3
Incident Response	1	0	1	2
Information Security Continuous Monitoring	0	0	0	0

Note: Totals do not equal the number of reports and testimonies identified because one report may cover several FISMA reporting metrics.

FISMA Metrics with the Most Frequently Reported Cybersecurity Weaknesses

In summarizing this year's 21 audit reports, we found that the cyber weaknesses most frequently cited, populated the FISMA metrics' categories of risk management, identity and access management, security and privacy training, contractor systems, and configuration management. The following report sections include examples from one or more of the 21 audit reports and describe how the cyber weaknesses negatively impact the DoD's cybersecurity mission. See Appendix B for a matrix of reports listed by their specific cybersecurity weaknesses and Appendix C for a list of reports summarized in this report.

Risk Management

Risk management for IT is the process of managing threats to organizational operations, organizational assets, other organizations, individuals, and the United States, that result from operating an information system. Risk management performance of a risk assessment,

- implementation of a risk mitigation strategy, and
- employment of techniques and procedures for the continuous monitoring of the information system's security.

The DoD audit community and the GAO reported risk management weaknesses in 13 reports and made 24 recommendations. Examples of those weaknesses are contained in the following two reports.

DoD Did Not Require Performance of Software Assurance Countermeasures
DoD OIG Report No. DODIG-2016-082, "DoD Needs to Require Performance of Software Assurance Countermeasures During Major Weapons Systems Acquisitions," April 29, 2016, identified that Littoral Combat Ship – Mission Modules program office officials did not ensure all software assurance countermeasures[3] detailed in the Program Protection Plan (PPP) were fully performed during software development. In July 2011, the Principal Deputy, Under Secretary of Defense for Acquisition, Technology, and Logistics (USD[AT&L]) issued a policy memorandum requiring all acquisition programs to develop a PPP to describe the program's critical areas, the related threats and vulnerabilities, and a plan to apply countermeasures to reduce associated risks. The PPP specifically includes software assurance countermeasures designed to reduce risk by verifying software functions as intended.

---

[3] Software assurance countermeasures are activities to counter adversarial threats that may target software.

According to the report, DoD policy did not require programs to perform all software assurance countermeasures contained in the PPP, and the DoD did not issue implementing procedures to ensure countermeasures were consistently applied across major acquisition programs. As a result, there was an increased risk that the Littoral Combat Ship – Mission Modules software contained vulnerabilities that, if exploited, could prevent the Littoral Combat Ship from performing its mission.

> There was an increased risk that … software contained vulnerabilities that … could prevent the Littoral Combat Ship from performing its mission.

The DoD OIG recommended that the USD(AT&L) develop and issue policy to require that program offices implement applicable software assurance countermeasures contained in their PPP. According to the report, the Acting Deputy Assistant Secretary of Defense for Systems Engineering, responding for the USD(AT&L), disagreed with the recommendation and stated that the recommended action was already completed with the reissuance of DoD Instruction 5000.02. The DoD OIG responded that while DoD Instruction 5000.02 was identified as the baseline software assurance policy, it does not contain implementation requirements. The DoD OIG also recommended that the USD(AT&L) develop and issue procedures to guide consistent application of software assurance countermeasures in PPPs. While the Acting Deputy agreed with the recommendation, the DoD OIG responded that the Acting Deputy did not address the specifics of the recommendation. The DoD OIG requested that the USD(AT&L) provide additional comments on both recommendations. In subsequent correspondence, USD(AT&L) personnel stated that revisions to existing software were planned for completion in December 2016.

Army Personnel Did Not Properly Manage Risks Associated with Task Critical Assets

(FOUO) ███
██
██
███
██
██
██
███
██

---
[4] ███
███████████████████████████████.

(FOUO) ███████████████████████████
████████████████████████████████████
████████████████████████████████
██
█████████████████████████████

(FOUO) ██████████████████████████████
█████████████████████████████████████
████████████████████████████████
██████████████████████████████████
███████████████████████████████████
██████████████████████████████████████
███████████████████████████████
████████████████████████████████████
██████████████████████████████████
████████████████████████████████████
██████████████████████████████████
██████████████████████████████████████
██
████████████████████████

(FOUO) ██████████████████████████
████████████████████████████████████
██████████████████████████████████
██
██████████████████████████████████
█████████████████████████████████████
████████████████████
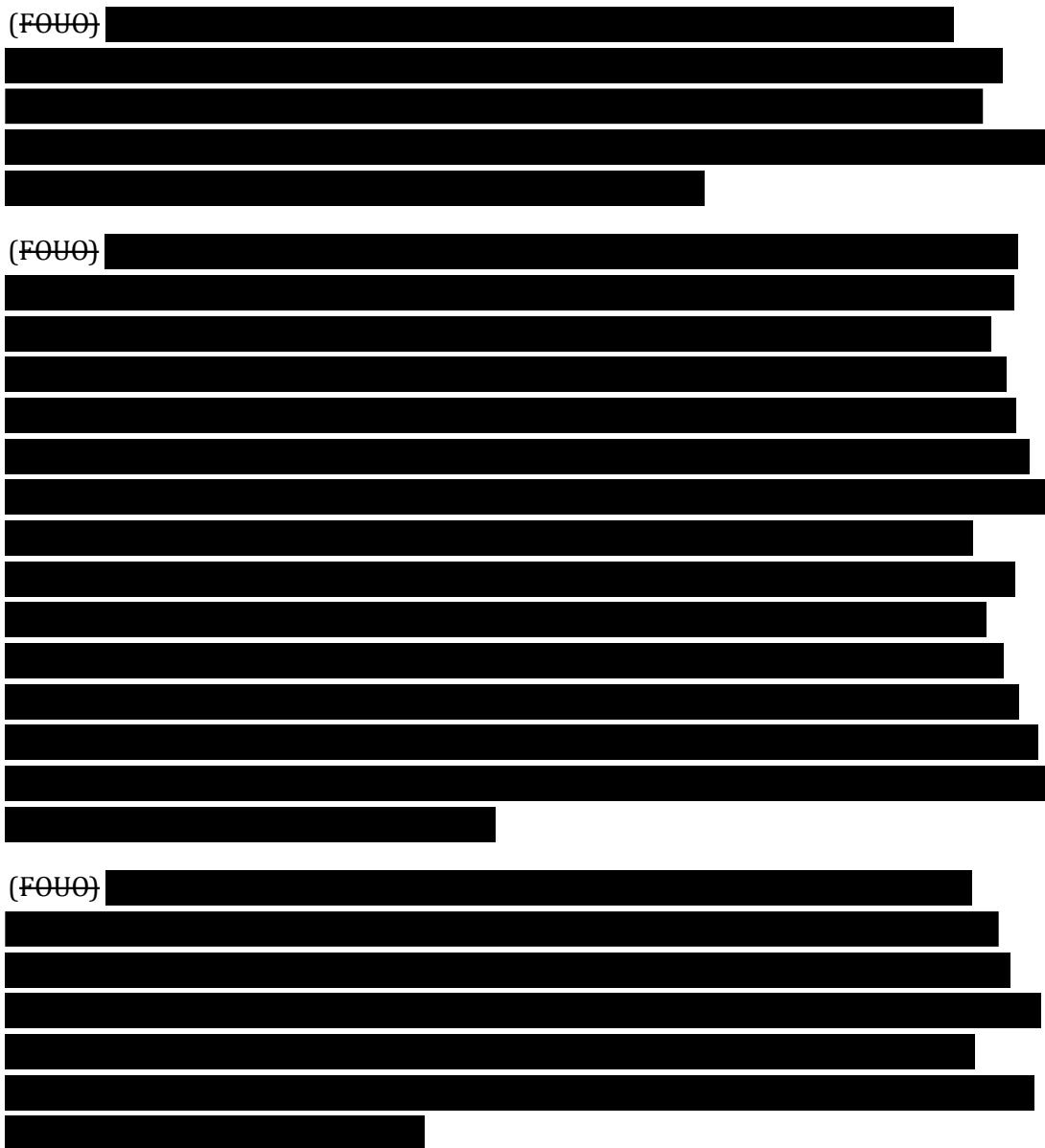
Identity and Access Management

Identity and access management includes the processes, technologies, and policies for managing digital identities and controlling how identities can be used to access resources. The DoD audit community and the GAO reported identity and access management weaknesses in 5 reports and made 26 recommendations. Examples of those weaknesses are contained in the following two reports.

---

[5] ███████████████████████████████

Air Force Personnel Did Not Review Account Access

Air Force Audit Agency Report No. F2016-0002-O10000, "Purchase Request Process System – Application Controls," March 30, 2016, identified that Purchase Request Process System (PRPS) program personnel did not effectively implement application control requirements necessary to achieve audit readiness. For example, PRPS personnel did not periodically review account access to ensure continued appropriateness as required, which allowed 510 out of 2,867 users with no requirement for access to have active accounts. Access controls limit or detect inappropriate access to computer resources, thereby protecting them from unauthorized modification, loss, and/or disclosure.

PRPS program personnel did not periodically review account access to ensure continued appropriateness as required because PRPS program management personnel did not implement the NIST Risk Management Framework. Instead, PRPS program personnel followed the pre-2014 DoD 8500-series policies that did not reflect current Federal regulations for application-level general, business process, interface, and data management controls. As a result, PRPS application control discrepancies cast doubt on the reliability of operational mission data used to generate purchase instruments. Additionally, audit costs and substantive testing sample sizes will increase if independent public accountants cannot rely on the system of internal controls supporting Air Force financial statements.

The Air Force Audit Agency recommended that the Commander, Air Force Materiel Command, implement internal control procedures to verify consistent and accurate compliance with Federal NIST system control standards detailed in DoD Instruction 8510.01. The Commander, Air Force Materiel Command, agreed and stated that the Air Force Materiel Command will develop a plan to modify PRPS to comply with Federal NIST standards, including risk management framework implementation in accordance with DoD Instruction 8510.01. Additionally, the Commander stated that the plan would include the implementation of internal control procedures to verify consistent and accurate compliance with the Federal NIST system control standards detailed in DoD Instruction 8510.01.

Army Activities Did Not Comply with Homeland Security Presidential Directive 12

(FOUO) ███████████████████████████
████████████████████████████████████
███████████████████████████████████
███████████████████████████████████
██████████████████████████████████
███████████████████████████████████
███████████████████████████████████
█████████████████████████
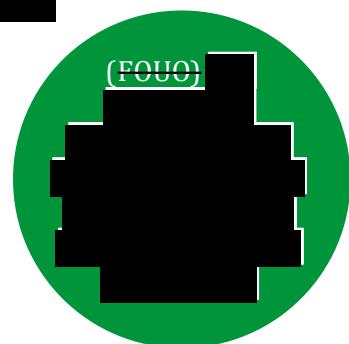
- (FOUO) ████████████████████████
  ██████████████

- (FOUO) ████████████████████████
  ████████████████████████████████ ;

- (FOUO) ████████████████████████
  ███████████████████

- (FOUO) ████████████████████████
  ██████████████ .

(FOUO) ████████████████████████████
████████████████████████████████████
██████████████████████████████

(FOUO) ████████████████████████████
██████████████████████████
███████████████████████████
██████████████████████████
████████████████████████████
██████████████████████████
███████████████████████████
██████████████████████████
████████████████████████████
█████████████████████

(FOUO)

- (FOUO) ████████████████████████
  ███████████████████ ,

- (FOUO) ████████████████████████
  ███████████████████

- (FOUO) ██████████████████████████████ .

(FOUO) ██
██
██
███
██
████████████████████████████████
██
██
███
██
████████████████
████████████████

(FOUO) ██
███
██
██
██
██
██
██
██
██
███████████████████████████████████

Security and Privacy Training

Security and privacy training includes the formal activities, products, and services intended to create or enhance the security knowledge or skills of personnel responsible for IT operations. The DoD audit community and the GAO reported security and privacy training weaknesses in five reports and made eight recommendations. Examples of those weaknesses are contained in the following two reports.

Navy Medical Providers Need to Improve Technical Safeguards for Personally Identifiable Information and Protected Health Information

(FOUO) ███████████████████████████████████████
███████████████████████████████████████
██
██
██

(FOUO) ██
██████████████████████████████████
███████████████████████████████
████████████████████████
█████████████████████████
███████████████████████
████████████████████████████
██████████████████████████████████
████████████████████████
███████████████████

(FOUO) ██████████████████████████████████████
██
██
██████████████████████████████████████
██████████████████████████████████████
██
██████████████████████████

(FOUO) ██
██
██
██
██

Army Portfolio Management Solution Contains Unreliable Data

Army Audit Agency Report No. A-2016-0062-IET, "Data Reliability in the Army Portfolio Management Solution," March 22, 2016, examined the Army Portfolio Management Solution (APMS), the Army's authoritative data source for information assurance and IT investments, to verify that the system had reliable data for senior leaders to make informed decisions. The report identified that data in APMS was not reliable despite having data fields to meet DoD and congressional requirements for IT portfolio management. Consequently, senior leaders used ineffective and inefficient methods to collect IT information. The Army Audit Agency reviewed 17 data fields related to portfolio management, funding, and information assurance and determined that all fields had inaccuracies or incomplete and illogical responses.

The report stated that this occurred because:

- users manually entered required data into APMS instead of leveraging interoperability with existing systems having the required data that was more definitive,

- guidance did not clearly define data elements or specific sources from which to obtain data to avoid varying interpretations of information requirements,

- training was not available to give users a clear understanding of the purpose and/or use of the data gathered, and

- controls were not effective to identify and remedy illogical or incomplete answers to data fields.

As a result, the Chief Information Officer/G-6, mission area IT portfolio managers, and commanders did not have reliable visibility over the Army's IT portfolio or network security, and they risked reporting inaccurate information to the DoD and Congress. Additionally, Army leaders could not leverage the big data analytical capability inherent in APMS due to the incomplete, unreliable conditions that existed.

The report recommended that the Chief Information Officer/G-6 develop training in the APMS so that system owners understand new guidance, new tools, and the purpose and/or use of the data gathered. The Chief Information Officer/G-6 agreed with the recommendation and stated that the office will publish an update to the APMS manual that would define the consumers and purpose of the data in APMS.

Contractor Systems

Contractor systems are information systems owned or operated by entities on behalf of the Federal Government, including systems that reside in the public cloud. The systems must meet the security requirements for all systems that process or store Federal Government information. The DoD audit community and the GAO reported contractor system weaknesses in four reports and made three recommendations. An example of this weakness is contained in the following report.

Air Force Communications Equipment Lacked Technical Support

(FOUO) ██████████████████████████████████████
██
██
██
██

(FOUO) ███████████████████████████████████
███████████████████████████████████
███████████████████████████████████
███████████████████████████████
███████████████████████████████████
███████████████

The inability to maintain consistent satellite connectivity occurred because headquarters AFRC personnel did not establish a standard process to ensure technical support for communications equipment. AFRC personnel did not continue a technical support contract for communications equipment and could not resolve operational problems due to the lack of proprietary technical expertise. Instead of continuing a previous technical support contract for communications equipment, AFRC headquarters personnel employed a SharePoint site to allow unit personnel to compare technical problems and troubleshoot solutions among themselves. However, this method could not resolve all operational problems due to the lack of proprietary technical expertise. For example, 5 of the 12 AFRC units were still reporting problems that required technical expertise during the support contract lapse.

(FOUO) ███████████████████████████████████
███████████████████████████████
███████████████████████████████████████
███████████████████████████████████
███████████████████

The Air Force Audit Agency recommended that the Air Force Reserve officials direct AFRC personnel to implement a standard process to ensure continued technical support for communications equipment. The Air Force Reserve officials agreed with the finding and recommendation and stated that AFRC/A6 re-established a technical support contract and that both contracting and plans and programs experts have integrated metrics for tracking the status of the support contract.

Configuration Management

Configuration management is a collection of activities focused on establishing and maintaining the integrity of IT products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle. The DoD audit community and the GAO reported configuration management weaknesses in three reports and made four recommendations. An example of this weakness is contained in the following report.

Air Force Project Management Resource Tools Were Not Properly Implemented

Air Force Audit Agency Report No. F2016-0001-O10000, "Project Management Resource Tools-General Controls," March 30, 2016, identified that Project Management Resource Tools (PMRT) personnel did not effectively implement security management, configuration management, and contingency planning general controls. The Assistant Secretary of the Air Force (Acquisition) provides the funding and personnel to maintain and deploy the PMRT. A service-level agreement between the Acquisition Integration, Acquisition Information Division, and the Army, Project Director, Acquisition, Logistics, and Technology Enterprise Systems and Services (ALTESS) provides network server hosting services for the production and operation of the PMRT. The agreement assigned physical, environmental, and network protection; maintenance of the operating system software on the servers; and backup support responsibilities to ALTESS. However, PMRT personnel remained responsible for all other general controls, including configuration management.

PMRT personnel did not effectively implement security management, configuration management, and contingency planning general controls because PMRT personnel did not initiate efforts to implement the requirements of the NIST Risk Management Framework and other Federal and DoD requirements. Instead, PMRT personnel followed expiring policy that did not reflect directed Federal regulations for general controls. Additionally, PMRT personnel did not establish ALTESS service-level agreement requirements to follow mandatory Federal standards for security-focused configuration management. Specifically, ALTESS personnel operated under a 2009 memorandum[6] that did not incorporate security-focused configuration management as required by the NIST. As a result, PMRT general control weaknesses cast doubt on the reliability of operation and financial data supporting the status of over 700 Air Force Acquisition projects and programs valued at over $40 billion. In addition, if independent public accountants cannot rely on the system of internal controls supporting Air Force financial statements, independent auditors will have to increase substantive testing sample sizes and increase the cost of audit accordingly.

---

[6] ALTESS memorandum 25-111, "Change Management Process," February 27, 2009.

The Air Force Audit Agency recommended that the Assistant Secretary of the Air Force (Acquisition) direct the Acquisition Integration, Acquisition Capability Division, to implement Federal NIST system control standards detailed in DoD Instruction 8510.01 and a 2013 memorandum from the Assistant Secretary of the Air Force (Financial Management and Comptroller).[7] This would include all applicable security management, configuration management, and contingency planning controls. Additionally, the Air Force Audit Agency recommended that the Assistant Secretary of the Air Force (Acquisition) direct the Acquisition Integration, Acquisition Capability Division to modify the ALTESS service-level agreement to require compliance with Federal NIST standards as detailed in DoD Instruction 8510.01, including development of a configuration management plan in accordance with NIST.[8] Management officials from the Assistant Secretary of the Air Force (Acquisition) agreed with the audit results and recommendations and stated that the Assistant Secretary of the Air Force (Acquisition) will direct the Acquisition Integration, Acquisition Capability Division, to implement Federal NIST system control standards and direct the Acquisition Integration, Acquisition Capability Division, to modify the ALTESS service-level agreement.

DoD's Progress to Implement Recommendations Reported in Previously Issued Cybersecurity Summary Reports

As of August 1, 2015, audit reports included in the previously issued cybersecurity summary reports contained 166 unresolved cybersecurity-related recommendations. From August 1, 2015, through July 31, 2016, DoD management closed 28 of those recommendations, leaving 138 unresolved cybersecurity-related recommendations that required management action. See the Figure for the issue date of reports containing the remaining 138 unresolved cybersecurity-related recommendations. See Appendix D for a list of the reports containing unresolved recommendations.

---

[7] Assistant Secretary of the Air Force (Financial Management and Comptroller) memorandum, "Information Technology – Financial Controls and Accounting Conformance Guidance," May 31, 2013.

[8] NIST Special Publication 800-128, "Guide for Developing Security Plans for Federal Information Systems," February 2006.

Figure. Issue Date of Reports Containing Unresolved Recommendations Related to Cybersecurity Weaknesses
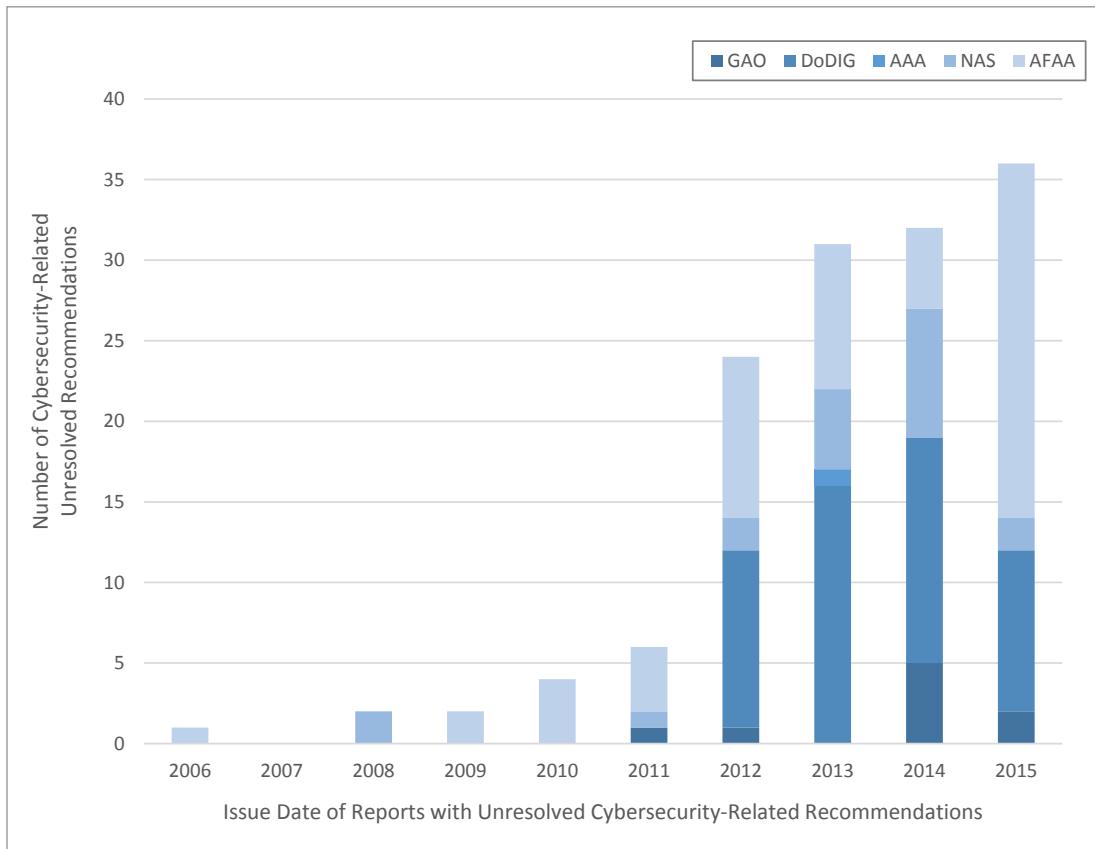
Cybersecurity Weaknesses Identified in Unresolved Recommendations

The most common cybersecurity weaknesses identified in the 138 unresolved recommendations relate to risk management, identity and access management, and contingency planning. Table 3 identifies the cybersecurity weaknesses as they relate to the unresolved recommendations.

Table 3. Cybersecurity Weaknesses Identified in Unresolved Recommendations

FISMA Reporting Metrics	GAO	DoD OIG	Military Departments	Total
Risk Management	3	20	54	77
Identity and Access Management	0	15	40	55
Contingency Planning	4	18	26	48
Configuration Management	2	9	17	28
Information Security Continuous Monitoring	0	4	14	18
Security and Privacy Training	0	4	6	10
Incident Response	0	3	3	6
Contractor Systems	0	3	0	3

Note: Totals do not equal the number of reports and testimonies identified because one report may cover several IG FISMA metrics.

Summary

The DoD has prioritized funding its cyber strategy by investing a total of $6.7 billion in FY 2017 and a total of $34.6 billion over the Future Years Defense Program (next five years). The funds are intended to help the DoD continue to develop, train, and equip the Cyber Mission Force, and make new technological investments to strengthen cyber defenses and capabilities. While the DoD has prioritized funding its cyber strategy, cybersecurity will continue to remain a significant management challenge. As recent audit reports identify, the DoD continues to face challenges in protecting and securing its networks, systems, and infrastructure from cyber threats and increasing its overall cyber capabilities. One of the most important challenges is the continuous effort to protect the DoD's systems and networks from increasingly sophisticated cyber-attacks.

The DoD audit community and the GAO issued 21 unclassified reports from August 1, 2015, through July 31, 2016, that identified cybersecurity weaknesses in one or more of the FY 2016 IG FISMA reporting metrics. The 21 reports demonstrated that the DoD continues to struggle with ensuring that all aspects of its information security program are adequately implemented. For example, implementing secure information systems on major weapons systems throughout their lifecycle requires effective and continuous software assurance testing. Inadequate software assurance testing on major weapons systems could be devastating to mission operations. In addition, although Homeland Security

Presidential Directive 12 was issued in 2004, one audit report indicated that DoD Components are still not fully complying with the Directive. The report identified the lack of compliance leaves national security and Privacy Act information vulnerable to compromise and places soldiers, family members, civilians, and critical infrastructures at greater risk of an adverse incident occurring.

The DoD audit community and the GAO attributed their findings to the lack of clear guidance and noncompliance with Federal and DoD guidance and identified recommended actions to correct the cybersecurity weaknesses and improve DoD cybersecurity. However, some of the recommendations are similar to recommendations cited in prior Cybersecurity Weaknesses Summary Reports. Therefore, not only must DoD Components take action in response to the report recommendations, the Components must also maintain the actions taken to decrease the risk of repeat findings.

Correcting cybersecurity weaknesses and maintaining adequate cybersecurity is critical, as the DoD has become increasingly reliant on cyberspace to enable its military, intelligence, and business operations to perform the full spectrum of military operations. Since 2013, the Director of National Intelligence has identified cyber threats as the top strategic global threat facing the United States. In addition, the GAO has identified cybersecurity of Federal information systems and networks as a high-risk area because all sectors of the Government—energy, transportation systems, communications, financial services, and defense of the homeland—are dependent on information systems and electronic data to perform operations and to process, maintain, and report essential information.

Appendix A

Scope and Methodology

We conducted this summary work from May 2016 through November 2016. We followed generally accepted government auditing standards, except for the standards of planning and evidence because the report summarizes previously released reports. This summary report supports the DoD OIG response to the requirements of Public Law 113-283, section 3555, "Federal Information Security Modernization Act of 2014," December 18, 2014.

This report summarizes the DoD cybersecurity weaknesses identified in 21 unclassified reports that the DoD audit community and the GAO issued from August 1, 2015, through July 31, 2016. To prepare this summary, we reviewed the websites of the GAO and each DoD Component audit organization and requested reports discussing cybersecurity weaknesses. We did not review the supporting documentation for any of the reports. This summary report does not contain recommendations because the summarized reports contained recommendations related to the cybersecurity weaknesses identified.

Use of Computer-Processed Data

We did not use computer-processed data to perform this audit.

Prior Coverage

During the last 5 years, the DoD OIG issued five reports summarizing cybersecurity weaknesses identified in 150 audit reports and testimonies issued by the DoD audit community and the GAO. Unrestricted DoD OIG reports can be accessed at http://www.dodig.mil/pubs/index.cfm. The following reports are For Official Use Only (FOUO) and can be obtained through the Freedom of Information Act Requestor Service website at https://www.dodig.mil/foia/submitfoia.html.

DoD OIG

Report No. DODIG-2015-180, "DoD Cybersecurity Weaknesses as Reported in Audit Reports Issued From August 1, 2014, Through July 31, 2015," September 25, 2015 (Report is FOUO)

Report No. DODIG-2014-126, "DoD Cybersecurity Weaknesses as Reported in Audit Reports Issued From August 1, 2013, Through July 31, 2014," September 26, 2014 (Report is FOUO)

Report No. DODIG-2013-141, "DoD Information Assurance Weakness as Reported by Audit Reports Issued From August 1, 2012, Through July 31, 2013," September 30, 2013 (Report is FOUO)

Report No. DODIG-2012-145, "DoD Information Assurance Weaknesses as Reported by Audit Reports Issued From August 1, 2011, Through July 31, 2012," September 27, 2012 (Report is FOUO)

Report No. D-2011-114, "Summary of Information Assurance Weaknesses as Reported by Audit Reports Issued From August 1, 2010, Through July 31, 2011," September 30, 2011

Appendix B

Matrix of Cybersecurity Weaknesses Reported From August 1, 2015, Through July 31, 2016

Agency Report No.	FY 2016 IG FISMA Metrics							
	Configuration Management	Contingency Planning	Contractor Systems	Identity and Access Management	Incident Response	Information Security Continuous Monitoring	Risk Management	Security and Privacy Training
Government Accountability Office								
GAO-16-332					X			
GAO-16-325			X					
GAO-16-79			X				X	
DoD Inspector General								
DODIG-2016-089							X	
DODIG-2016-082							X	
DODIG-2016-068	X						X	
DODIG-2016-054				X				
DODIG-2016-038			X				X	
Army Audit Agency								
A-2016-0116-IET							X	
A-2016-0088-IET				X				
A-2016-0062-IET							X	X
A-2016-0043-IEP					X		X	X
A-2016-0011-IET							X	
A-2016-0001-IEP				X				
Naval Audit Service								
N2016-0038							X	
N2016-0035								X
N2016-0013				X			X	X

Matrix of Cybersecurity Weaknesses Reported From August 1, 2015, Through July 31, 2016 (cont'd)

Agency Report No.	FY 2016 IG FISMA Metrics							
	Configuration Management	Contingency Planning	Contractor Systems	Identity and Access Management	Incident Response	Information Security Continuous Monitoring	Risk Management	Security and Privacy Training
Air Force Audit Agency								
F2016-0001-O10000	X	X						
F2016-0002-O10000	X	X		X			X	
F2015-0007-O40000		X	X					X
F2015-0011-O10000							X	
Total	**3**	**3**	**4**	**5**	**2**	**0**	**13**	**5**

Note: Totals do not equal the number of reports and testimonies identified because one report may cover several IG FISMA metrics.

Appendix C

Audit Reports Issued From August 1, 2015, Through July 31, 2016

Unrestricted GAO reports can be accessed at http://www.gao.gov. Unrestricted Army Audit Agency reports can be accessed at https://www.aaa.army.mil/. Naval Audit Service reports and Air Force Audit Agency reports are unavailable over the Internet. Unrestricted DoD OIG reports can be accessed at http://www.dodig.mil/pubs/index.cfm.

GAO

Report No. GAO-16-332, "Civil Support: DoD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities During Cyber Incidents," April 2016

Report No. GAO-16-325, "Cloud Computing: Agencies Need to Incorporate Key Practices to Ensure Effective Performance," April 2016

Report No. GAO-16-79, "Critical Infrastructure Protection: Sector-Specific Agencies Need to Better Measure Cybersecurity Progress," November 2015

DoD OIG

Report No. DODIG-2016-089, "Followup Audit: Audit Recommendations From Report No. DODIG-2013-109 Were Not Fully Implemented, but Controls Were in Place to Prevent Unauthorized Access to Robert C. Byrd and Greenup Locks and Dams," May 10, 2016 (Report is FOUO)

Report No. DODIG-2016-082, "DoD Needs to Require Performance of Software Assurance Countermeasures During Major Weapon System Acquisitions," April 29, 2016 (Report is FOUO)

Report No. DODIG-2016-068, "DoD's Efforts to Consolidate Data Centers Need Improvement," March 29, 2016

Report No. DODIG-2016-054, "Navy Controls for Invoice, Receipt, Acceptance, and Property Transfer System Need Improvement," February 25, 2016

Report No. DODIG-2016-038, "DoD Needs an Effective Process to Identify Cloud Computing Service Contracts," December 28, 2015

Army Audit Agency

Report No. A-2016-0116-IET, "Audit of the Defense Research and Engineering Network Security," July 27, 2016 (Report is FOUO)

Report No. A-2016-0088-IET, "Followup Audit of Elevated Privileges," May 3, 2016

Report No. A-2016-0062-IET, "Data Reliability in the Army Portfolio Management Solution," March 22, 2016

Report No. A-2016-0043-IEP, "Army Tier 2 and Tier 3 Critical Infrastructure Risk Management Program," February 25, 2016 (Report is FOUO)

Report No. A-2016-0011-IET, "Audit of Nontactical Mobile Applications," December 1, 2015

Report No. A-2016-0001-IEP, "Uncleared Contractor Credentialing and Installation Access Controls," October 16, 2015 (Report is FOUO)

Naval Audit Service

Report No. N2016-0038 "Approval of Marine Corps Travel Vouchers in the Defense Travel System," June 30, 2016 (Report is FOUO)

Report No. N2016-0035 "Defense Travel System Approving Officials' Approval of Travel Vouchers at Norfolk Naval Shipyard," June 2, 2016 (Report is FOUO)

Report No. N2016-0013 "Managing Personally Identifiable Information at Naval Medical Center, Portsmouth and Naval Hospital, Jacksonville," December 29, 2015 (Report is FOUO)

Air Force Audit Agency

Report No. F2016-0001-O10000, "Project Management Resource Tools-General Controls," March 30, 2016

Report No. F2016-0002-O10000, "Purchase Request Process System – Application Controls," March 30, 2016

Report No. F2015-0007-O40000, "Selected Aspects of Air Force Reserve Command Cyberspace Career Field Management," September 4, 2015 (Report is FOUO)

Report No. F2015-0011-O10000, "Command and Control Platform Information Technology Security," September 4, 2015

Appendix D

Audit Reports From Prior Cybersecurity Summary Reports With Unresolved Recommendations

As of August 1, 2015, previously identified audit reports contained 166 unresolved cybersecurity-related recommendations. During the reporting period of August 1, 2015, through July 31, 2016, management resolved 28 recommendations, leaving 138 unresolved cybersecurity-related recommendations. These 138 unresolved recommendations are contained in the 59 audit reports listed in this Appendix. The list of reports with unresolved recommendations was compiled based on information the DoD audit community and the GAO provided in August 2016 and may be incomplete because of the extent of information maintained in their respective followup systems.

Unrestricted GAO reports can be accessed at http://www.gao.gov. Unrestricted Army Audit Agency reports can be accessed at https://www.aaa.army.mil/. Naval Audit Service reports and Air Force Audit Agency reports are unavailable over the Internet. Unrestricted DoD OIG reports can be accessed at http://www.dodig.mil/pubs/index.cfm.

GAO

Report No. GAO-15-544, "Insider Threats: DoD Should Strengthen Management and Guidance to Protect Classified Information and Systems," June 2015

Report No. GAO-14-404SU, "Defense Cybersecurity: DoD Needs to Better Plan for Continuity of Operations in a Degraded Cyber Environment and Provide Increased Oversight," April 2014 (Report is FOUO)

Report No. GAO-14-182, "Defense Logistics: Actions Needed to Improve Department-Wide Management of Conventional Ammunition Inventory," March 2014

Report No. GAO-12-992, "VA and DoD Health Care: Department-Level Actions Needed to Assess Collaboration Performance, Address Barriers, and Identify Opportunities," September 2012

Report No. GAO-11-421, "Defense Department Cyber Efforts: More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities," May 2011

DoD OIG

Report No. DODIG-2015-102, "Additional Actions Needed to Effectively Reconcile Navy's Fund Balance With Treasury Account," April 3, 2015

Report No. DODIG-2015-045, "DoD Cloud Computing Strategy Needs Implementation Plan and Detailed Waiver Process," December 4, 2014

Report No. DODIG-2015-044, "DoD Needs to Reinitiate Migration to Internet Protocol Version 6," December 1, 2014 (Report is FOUO)

Report No. DODIG-2015-008, "Followup Audit: Enterprise Blood Management System Not Ready for Full Deployment," October 23, 2014

Report No. DODIG-2014-066, "Logistic Modernization Program System Not Configured to Support Statement of Budgetary Resources," May 5, 2014

Report No. DODIG-2014-037, "Systemic Weaknesses Leave Civil Works Infrastructure Vulnerable to Physical and Cyber Attacks," February 10, 2014 (Report is FOUO)

Report No. DODIG-2013-142, "DoD Evaluation of Over-Classification of National Security Information," September 30, 2013

Report No. DODIG-2013-134, "Navy Commercial Access Control System Did Not Effectively Mitigate Access Control Risks," September 16, 2013 (Report is FOUO)

Report No. DODIG-2013-130, "Army Needs to Improve Controls and Audit Trails for the General Fund Enterprise Business System Acquire-to-Retire Business Process," September 13, 2013

Report No. DODIG-2013-072, "Data Loss Prevention Strategy Needed for the Case Adjudication Tracking System," April 24, 2013 (Report is FOUO)

Report No. DODIG-2013-036, "Improvements are Needed to Strengthen Security Posture of USACE, Civil Works, Critical Infrastructure and Industrial Control Systems in the Northwestern Division," January 14, 2013 (Report is FOUO)

Report No. DODIG-2012-122, "DoD Should Procure Compliant Physical Access Control Systems to Reduce the Risk of Unauthorized Access," August 29, 2012 (Report is FOUO)

Report No. D-2012-090, "Improvements Needed to Strengthen the Defense Enrollment Eligibility Reporting System Security Posture," May 22, 2012 (Report is FOUO)

Report No. D-2012-050, "Improvements Needed With Host-Based Intrusion Detection Systems," February 3, 2012 (Report is FOUO)

Army Audit Agency

Report No. A-2013-0130-FMR, "Miscellaneous Pay Process General Fund Enterprise Business System," July 31, 2013

Naval Audit Service

Report No. N2015-0027, "Followup on Naval Audit Service Report N2012-0009, "Personally Identifiable Information and Department of the Navy Data on Unencrypted Computer Hard Drives Released from Department of the Navy Control," July 23, 2015 (Report is FOUO)

Report No. N2015-0026, "Management Controls of Navy Corporate Data," July 16, 2015 (FOUO)

Report No. N2014-0029, "Internal Controls for Overtime Benefits Received at Norfolk Naval Shipyard and Portsmouth Naval Shipyard," July 1, 2014 (Report is FOUO)

Report No. N2014-0022, "Fleet Gapped Critical Billets," May 20, 2014 (Report is FOUO)

Report No. N2014-0021, "Cyberspace/Information Technology Skill Sets for Active Duty Military Personnel at Selected Navy Commands," May 19, 2014 (Report is FOUO)

Report No. N2013-0050, "Long-Term Temporary Duty Orders for Marine Corps Reserves Performing Duty within the Continental United States and Hawaii," September 30, 2013 (Report is FOUO)

Report No. N2012-0070, "Navy Compliance with Department of Defense Information Assurance Certification and Accreditation Process," September 28, 2012 (Report is FOUO)

Report No. N2011-0046, "Followup of Management of Personally Identifiable Information at Marine Corps Recruiting Command," July 29, 2011 (Report is FOUO)

Report No. N2008-0023, "Information Security within the Marine Corps," February 20, 2008

Air Force Audit Agency

Report No. F2015-0010-O10000, "Depot Maintenance and Production System-Time and Attendance Application Controls," April 2, 2015

Report No. F2015-0009-O10000, "Stock Control System Application Controls," April 2, 2015

Report No. F2015-0008-O10000, "Military Personnel Data System Application Controls," March 10, 2015

Report No. F2015-0007-O10000, "Standard Procurement System Application Controls," March 10, 2015

Report No. F2015-0006-O10000, "Commanders Resource Integration System Application Controls," March 10, 2015

Report No. F2015-0005-O10000, "Contract Writing System Application Controls," March 10, 2015

Report No. F2015-0004-O10000, "Automated Contract Preparation System Application Controls," March 10, 2015

Report No. F2015-0001-O1000, "Cargo Movement Operations System Application Controls," December 15, 2014

Report No. F2014-0004-O10000, "Memorandum Report of Audit F2014-0004-O10000, Automated Contract Preparation System General and Application-Level General Controls," November 1, 2013

Report No. F2014-0003-O10000, "Memorandum Report of Audit F2014-0003-O10000, Integrated Logistics System-Supply Application Controls," November 1, 2013

Report No. F2014-0005-O10000, "Standard Procurement System General and Selected Application Controls," December 3, 2013

Report No. F2013-00016-O40000, "Memorandum Report of Audit F2013-0016-O40000, Reserve Travel System – Phase 1, General and Selected Application Controls," September 5, 2013

Report No. F2013-0005-O10000, "Enterprise Information Protection Capability," October 26, 2012

Report No. F2013-0003-L20000, "Serialized Parts Configuration Management," April 1, 2013

Report No. F2013-0011-O10000, "Memorandum Report of Audit F2013-0011-O10000, Integrated Missile Database System Application Controls," January 15, 2013

Report No. F2013-0009-O10000, "Memorandum Report of Audit F2013-0009-O10000, Reliability, Availability, Maintainability Support System for Electronic Combat Pods-Application Controls," January 3, 2013

Report No. F2013-0007-O10000, "Memorandum Report of Audit F2013-0007-O10000, Financial Inventory Accounting and Billing System Application Controls," November 20, 2012

Report No. F2013-0003-O10000, "Memorandum Report of Audit F2013-0003-O10000, Reliability and Maintainability Information System Application Controls," October 22, 2012

Report No. F2012-0009-FB2000, "Memorandum Report of Audit F2012-0009-FB2000, Automated Funds Management General Controls," June 26, 2012

Report No. F2012-0006-FB2000, "Memorandum Report of Audit F2012-0006-FB2000, Positive Inventory Control Fusion - Application Controls," April 12, 2012

Report No. F2012-0005-FB2000, "Memorandum Report of Audit F2012-0005-FB2000, Automated Funds Management Application Controls," April 4, 2012

Report No. F2012-0003-FB4000, "System Vulnerability Detection and Mitigation," February 16, 2012

Report No. F2012-0003-FB2000, "Defense Enterprise Accounting and Management System Selected System Controls," January 17, 2012

Report No. F2012-0002-FB4000, "Air National Guard Information Systems Security," January 11, 2012

Report No. F2011-0004-FB4000, "Computer Network Incident Response and Reporting," April 20, 2011

Report No. F2010-0009-FB2000, "Implementation of Chief Financial Officer Compliance Tracking for Financial Systems," July 28, 2010

Report No. F2010-0005-FB4000, "Publicly Accessible Air Force Web Sites," May 14, 2010

Report No. F2009-0007-FD4000, "Personnel Security Clearances," May 8, 2009

Report No. F2009-0004-FB2000, "Defense Enterprise Accounting and Management System Controls," February 20, 2009

Report No. F2006-0006-FB2000, "Controls for the Wholesale and Retail Receiving and Shipping System," May 19, 2006

Glossary

Configuration Management: the management of security features and assurances through control of changes made to hardware, software, firmware, documentation, test, test fixtures, and test documentation throughout the life cycle of an information system.

Contingency Planning: the process of preparing for emergency response, backup operations, and post-disaster recovery of an information system to ensure the availability of critical resources and to facilitate the continuity of operations in an emergency.

Contractor Systems: agency systems operated on the agency's behalf by contractors or other entities, including agency systems and services residing in a cloud external to the agency.

Identity and Access Management: the processes, technologies, and policies for managing digital identities and controlling how identities can be used to access resources.

Incident Response: the mitigation of violations of security policies and recommended practices; also referred to as incident handling.

Information Security Continuous Monitoring: maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

Risk Management: the process of managing threats to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organization, and the Nation, resulting from information system operations, and includes:

- the performance of a risk assessment,
- the implementation of a risk mitigation strategy,
- employment of techniques and procedures for the continuous monitoring of the information system's security state, and
- documenting of the overall risk management program.

Security and Privacy Training: formal activities, products, and services intended to create or enhance the security knowledge or skills of persons or raise their level of performance, motivation, or operations.

Acronyms and Abbreviations

AFRC	Air Force Reserve Command
ALTESS	Acquisition, Logistics, and Technology Enterprise Systems and Services
APMS	Army Portfolio Management Solution
CAC	Common Access Card
CIRM	Critical Infrastructure Risk Management
FISMA	Federal Information Security Modernization Act
GAO	Government Accountability Office
IT	Information Technology
NHJAX	Naval Hospital, Jacksonville
NIST	National Institute of Standards and Technology
NMCP	Naval Medical Center, Portsmouth
PHI	Protected Health Information
PII	Personally Identifiable Information
PMRT	Project Management Resource Tools
PPP	Program Protection Plan
PRPS	Purchase Request Process System
SMADS	Strategic Mission Assurance Data System
TCA	Task Critical Asset
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics

Whistleblower Protection
U.S. Department of Defense

The Whistleblower Protection Ombudsman's role is to educate agency employees about prohibitions on retaliation and employees' rights and remedies available for reprisal. The DoD Hotline Director is the designated ombudsman. For more information, please visit the Whistleblower webpage at www.dodig.mil/programs/whistleblower.

For more information about DoD IG reports or activities, please contact us:

Congressional Liaison
congressional@dodig.mil; 703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

For Report Notifications
www.dodig.mil/pubs/email_update.cfm

Twitter
www.twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline

DEPARTMENT OF DEFENSE | INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, VA 22350-1500
www.dodig.mil
Defense Hotline 1.800.424.9098